BLACKBIRD FOR TRAINING

Incident Response and Digital Forensics

29 March – 2 April 2027
Kuala Lumpur (Malaysia)

UK Traininig
PARTNER



Incident Response and Digital Forensics

Ref: 3255278_337023 **Date:** 29 March – 2 April 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction

In today's hyperconnected digital world, cyberattacks are not a matter of if but when. As organizations increasingly depend on digital infrastructure, the ability to respond effectively to security incidents and investigate them thoroughly has become a critical business capability. Incident Response and Digital Forensics form the cornerstone of modern cybersecurity resilience — enabling organizations to detect, contain, and recover from security breaches while preserving vital evidence for analysis.

The Incident Response and Digital Forensics course provides participants with a comprehensive understanding of how to identify, analyze, and mitigate cyber incidents through structured methodologies and hands-on tools. It combines the theoretical frameworks of incident response with the technical depth of digital forensics, ensuring professionals can act decisively during and after cyber crises.

This course is designed for cybersecurity specialists, IT administrators, SOC analysts, and digital investigation professionals who seek to strengthen their response readiness, enhance forensic analysis capabilities, and ensure data integrity across digital platforms.

Course Objectives

By the end of this course, participants will be able to:

- Understand the principles and lifecycle of incident response.
- Develop and implement an effective incident response plan.
- Identify indicators of compromise and detect ongoing attacks.
- Apply digital forensic techniques to preserve and analyze evidence.
- Conduct detailed investigations of compromised systems.
- Utilize forensic tools to collect, analyze, and report digital evidence.
- Integrate incident response with organizational cybersecurity strategies.
- Document findings for legal, technical, and management purposes.



Course Outlines

Day 1: Fundamentals of Incident Response and Cyber Threats

- Introduction to incident response frameworks and standards e.g., NIST, SANS.
- Understanding types of cyber incidents: malware, ransomware, and insider threats.
- The incident response lifecycle: preparation, identification, containment, eradication, recovery, and lessons learned.
- Roles and responsibilities of the incident response team.
- Key elements of an effective incident response policy.

Day 2: Incident Detection and Analysis

- Identifying early warning signs and indicators of compromise IOCs.
- Techniques for log analysis and event correlation.
- Utilizing SIEM tools for real-time detection.
- Differentiating between false positives and genuine threats.
- Performing threat intelligence integration for enhanced visibility.

Day 3: Digital Forensics Fundamentals

- Principles of digital forensics and evidence preservation.
- Understanding data acquisition and the chain of custody.
- Disk and memory imaging techniques.
- File system analysis and metadata extraction.
- Forensic tools and software overview e.g., EnCase, Autopsy, FTK.

Day 4: Forensic Investigation and Incident Containment

- Investigating compromised systems and recovering deleted data.
- Malware analysis and tracing attacker activities.
- Network forensics: packet analysis, intrusion tracing, and traffic reconstruction.
- Incident containment and eradication strategies.
- Coordinating incident response across departments and systems.

Day 5: Reporting, Recovery, and Post-Incident Review

- Writing professional forensic and incident response reports.
- Documenting findings for compliance and legal admissibility.
- Communicating technical results to non-technical stakeholders.
- Building long-term recovery and resilience plans.
- Conducting post-incident reviews and implementing lessons learned.



Why Attend This Course: Wins & Losses!

- Gain a deep understanding of modern cyber incident response frameworks.
- Learn practical digital forensics methods to investigate and contain attacks.
- Acquire hands-on experience with forensic tools and data analysis techniques.
- Enhance your ability to preserve, collect, and interpret digital evidence.
- Improve coordination between technical and management response teams.
- Strengthen compliance with cybersecurity regulations and standards.
- Build organizational resilience and readiness against cyber threats.
- Develop the confidence to lead incident response operations effectively.

Conclusion

The Incident Response and Digital Forensics course equips professionals with the skills to manage cyber crises with precision, confidence, and accountability. In a threat landscape where attackers are becoming increasingly sophisticated, the ability to respond rapidly and analyze incidents thoroughly is no longer optional — it is essential.

This masterclass integrates practical scenarios, tool-based exercises, and real-world methodologies to help participants anticipate, detect, and mitigate cyber incidents while ensuring data integrity and operational continuity.

By mastering both incident response and digital forensics, professionals become vital defenders of their organizations' digital assets — capable of turning every incident into an opportunity to enhance security maturity and strategic resilience.v

